REMARKS

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-47 are currently pending in the subject application and are presently under consideration. Claims 1-9, 12-17, 19, 23, 25-41, 46, and 47 have been amended as shown on pages 5-14 of the Reply. New claims 48-50 have been added. Also, the specification has been amended as shown on pages 2-4.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-47 Under 35 U.S.C. §103(a)

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-47 stand rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Swiler, *et al.* (US 7,013,395) in view of Townsend (U.S 6,374,358). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Swiler, *et al.* and Townsend, individually or in combination, do not disclose all features of the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j). See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. ____, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

One or more embodiments of the present application relate to security analysis and validation in an industrial automation environment. A security analysis tool can receive an abstract description or model of an automation system and perform a security assessment on the system. The tool can then generate security outputs that mitigate possible security concerns anticipated by the tool given the abstract description of the system. These security outputs can include system-specific recommendations for additional security components, procedures,

settings, topologies and the like. The outputs can also include automated security actions that can be deployed to components on the system to automatically adjust security parameters or add/remove security components based on the results of the analysis. In particular, amended independent claim 1 recites, *an interface component that generates a description of one or more industrial controllers, wherein the description includes at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, or wireless access patterns; an analyzer component that* ***generates one or more security outputs based on the description****, the one or more security outputs including at least one output* ***deployed to the one or more industrial controllers that adjusts a security parameter associated with the one or more industrial controllers****.*

Swiler, *et al.* does not disclose or suggest these aspects. Swiler, *et al.* relates to an analysis tool that assesses potential security risks in a network and generates an "attack graph" that graphically illustrates possible attack paths that could be taken by a malicious entity. However, the cited reference merely proposes *displaying* this attack graph graphically to a user for analysis purposes, and does not contemplate deploying any type of output to an industrial controller as a result of the analysis, or making any manner of parameter adjustment to the controller. As such, Swiler, *et al.* does not disclose generating one or more security outputs based on a description of one or more industrial controllers, or deploying at least one of these security outputs to the one or more industrial controllers to *adjust a security parameter associated with the one or more industrial controllers*.

Townsend is also silent regarding these aspects. Townsend relates to a method for assessing the effectiveness of respective network security countermeasures. According to Townsend's method, business concerns, potential network attack types, and possible countermeasures are compiled, and each countermeasure is analyzed with respect to each attack type for cost and effectiveness. However, like Swiler, *et al.*, Townsend does not deploy outputs to, or otherwise alter, devices on the network being assessed. Rather, Townsend merely outputs a written report of the assessment that includes a recommendation for countermeasure implementation (see column 8, lines 1-13). Consequently, Townsend fails to remedy the deficiencies of Swiler, *et al.* with respect to *generating one or more security outputs* based on a description of one or more industrial controllers, including at least one output *deployed to the*

one or more industrial controllers that adjusts a security parameter associated with the one or more industrial controllers.

Likewise, amended independent claim 17 recites, *a validation component that automatically assesses security capabilities of the industrial automation device based upon a comparison of the security related data and one or more predetermined security guidelines; a security analysis tool that recommends interconnection of one or more industrial automation devices to achieve a specified security goal; and* ***a component that automatically adjusts at least one security parameter in the industrial automation device in response to detected security event.*** As discussed *supra*, neither Swiler, *et al*. nor Townsend contemplate performing any manner of automated adjustments to an industrial device, and therefore fail to disclose or suggest adjustment of a security parameter in an industrial automation device in response to detected security events.

Similarly, amended independent claim 26 recites, *scanning one or more industrial automation devices for potential security violations at periodic intervals, wherein identity information about end devices having potential for hacker entry is gained;* ***performing an automated security procedure that adjusts at least one security parameter on the one or more industrial automation devices based at least in part on the potential security violations.*** The cited references are silent regarding these aspects, as noted above.

Also, amended independent claim 30 recites, *means for scanning one or more industrial automation devices for potential security violations; means for* ***initiating a security procedure that adjusts at least one security parameter in the one or more industrial automation devices in response to the potential security violations***, and as already discussed, Swiler, *et al*. and Townsend fail to disclose these features.

Amended independent claim 31 recites, *a detection component that automatically triggers a security event based upon detected deviations of subsequent industrial automation activities after the training period, wherein the* ***security event includes adjusting at least one security parameter associated with the industrial automation environment.*** As noted *supra*, Swiler, *et al*. and Townsend fail to disclose or suggest these aspects.

In addition to the features already discussed, one or more embodiments of the subject application can monitor network access to devices on the network during a training period to learn access patterns with respect to the devices. The network access can then be monitored

subsequent to the training period in order to detect deviations from the learned access patterns. Such deviations outside a predetermined threshold can cause a security event to be performed in response to the deviation. In particular, amended independent claim 12 recites, *monitoring access to the one or more industrial controllers for a predetermined training period to learn at least one access pattern; and* ***performing at least one automated security event if a detected deviation from the at least one access pattern exceeds a tolerance after the training period***.

With regard to access patterns, the Office Action contends generally that Swiler, *et al.* "clearly deal[s] with Intranet and Internet access patterns insofar as network security *per se* is concerned" (page 5 of the Office Action), ostensibly asserting that evaluating potential weaknesses in network security inherently deals with access patterns generally. However, even assuming *arguendo* that this is the case with the network security analysis tool of Swiler, *et al.*, a general assessment of Intranet and Internet access patterns nevertheless fails to suggest the more specific aspects of detecting *if a detected deviation from an access pattern exceeds a tolerance after a training period*, or performing at least one automated security event if such a deviation is detected. Swiler, *et al.* nowhere discloses performing a security event based on such criteria. Townsend also fails to disclose these aspects, as that cited reference is also silent regarding monitoring of access patterns generally, and more specifically is silent regarding *performing at least one automated security event if a detected deviation from at least one access pattern exceeds a tolerance after a training period.*

Moreover, the above-mentioned automated security events can, in one or more embodiments of the present application, serve to alter a current access pattern when a deviation from a learned access pattern in excess of a threshold is detected. In this way, a positive action is automatically performed to mitigate potential access-related security threats. To this end, amended independent claim 16 recites, *means for* ***automatically detecting a deviation from the at least one access pattern that exceeds a threshold****; and means for performing an automated action that* ***alters a current access pattern based at least in part on the detected deviation.*** As discussed above, Swiler, *et al.* and Townsend do not disclose or suggest detecting a deviation from at least one access pattern that exceeds a threshold, or performing an automated action based on such a detected deviation. Consequently, the cited references fail to disclose more specifically that such an automated action can serve to *alter a current access pattern* based on the detected deviation. Indeed, the cited references are silent regarding any type of automated

corrective security measure performed on a network, as discussed above, and it therefore cannot be said that Swiler, *et al.* and Townsend, individually or in combination, disclose the specific actions set forth in amended independent claim 16, or the pattern-based criteria for triggering such actions.

Similarly, amended independent claim 39 recites, *monitoring a network of industrial controllers for a predetermined time; automatically learning at least one data transfer pattern of the network of industrial controllers during the predetermined time;* ***generating an alarm and altering network activity to adjust a current data transfer pattern if the current data transfer pattern is determined to be outside of a predetermined threshold.*** The cited references fail to disclose or suggest these features, as noted above.

Amended independent claim 41 recites, *means for scanning a network; means for learning access patterns to at least one industrial automation device from the network; and means for* ***generating a security event that disables network requests from at least one outside network upon determining that the access patterns are out of tolerance with stored access patterns***. As already discussed, Swiler, *et al.* and Townsend do not disclose generation of a security event upon determining that an access pattern has deviated from a learned access pattern. Nor do the cited references disclose generating such a security event upon determining that an access pattern is out of tolerance with a *stored* access pattern of any kind. Moreover, neither Swiler, *et al.* nor Townsend disclose that such a security event can specifically serve to *disable network requests from at least one outside network*, since the cited references do not perform a direct action of any kind on a system under analysis, as noted *supra*.

Amended claim 15 recites, *automatically deploying the one or more security outputs to the one or more industrial controllers; or utilizing the one or more security outputs to mitigate at least one of unwanted network access or network attack*. As already discussed, neither Swiler, *et al.* nor Townsend deploy any manner of security outputs to industrial controllers.

Also, amended claim 40 recites, *employing the at least one data transfer pattern as input for a security analysis process; and* ***adjusting at least one security parameter associated with the network of industrial controllers based on the security analysis process and the input***. The cited references fail to disclose adjustment of a security parameter associated with a network of industrial controllers, as discussed above.

Furthermore, one or more embodiments of the subject application provide for automatic installation of security components based on vulnerabilities detected as a result of analyzing a description of one or more controllers. In particular, new claim 48 recites, *the validation component automatically installs one or more security components in response to the one or more vulnerabilities*. The cited references, which merely output reports or graphs as a result of a network security assessment, do not disclose or suggest automatic installation of a security component as a result of one or more determined vulnerabilities. Although the Office Action states on page 3 that "it would have been obvious...for the adaptive countermeasure selection method/apparatus of Townsend to be combined with the validation component vulnerability assessment results of Swiler *et al*., insofar as the Swiler *et al*. teaching of a computer system analysis tool requiring a responding mechanism to make use of the analysis tool output (*i.e.*, the Townsend countermeasure selection method/***apparatus installation countermeasures aspect***...), and would be in itself an obvious intended use," it is noted that, contrary to this assertion, Townsend does not include an "apparatus installation countermeasures aspect." Rather, as already observed, the cited reference merely produces a written report as output, and does not perform an installation of any type of component.

Furthermore, new claim 49 recites, *the analyzer component further performs an automated action that alters access patterns to the one or more industrial controllers upon detecting a deviation from the at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, or wireless access patterns in excess of a threshold*, while new claim 50 recites, *the at least one automated security event includes at least disabling network attempts to access the one or more industrial controllers*. As discussed *supra*, neither Swiler, *et al*. nor Townsend disclose these features.

In view of at least the foregoing, it is respectfully submitted that Swiler, *et al*. and Townsend, individually or in combination, do not disclose or suggest all aspects of amended independent claims 1, 12, 16, 17, 26, 30, 31, 39, and 41 (and all claims depending there from), and as such fail to make obvious the present invention. It is therefore requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731